mississippi department of
Information Technology Services

3771 Eastwood Drive
Jackson, MS 39211-6381
Phone: 601-432-8000
Fax: 601-713-6380
www.its.ms.gov

Craig P. Orgeron, Ph.D., Executive Director

LOC Questions and Clarifications Memorandum

To: Solicited Vendors for Letter of Configuration (LOC) Number 41784, dated March 3, 2014 for the Mississippi Department of Revenue (DOR)

From: Craig P. Orgeron, Ph.D.

Date: April 16, 2015

Subject: Responses to Questions Submitted and Clarifications to Specifications

Contact Name: Patti Irgens

Contact Phone Number: 601-432-8223

Contact E-mail Address: Patti.Irgens@its.ms.gov

LOC Number 41784 is hereby amended as follows:

1. Section 5 DOR NETWORK ENVIRONMENT is being modified as follows:

5.2.1 DOR utilizes two logical firewalls to segment their network segments. The primary firewall is a Cisco ASA ~~5585x~~**5520** located at DOR HQ. This firewall is in front of DOR HQ, DOR remote sites, and all DOR servers not behind the second firewall. The second firewall is a context in a Cisco ASA-SM. This context is in front of the DOR servers that are hosted in the State Data Center that make up part of the DOR MARS project. Work is underway to migrate off of our physical Cisco ASA at the DOR HQ, to ~~a context in the Cisco ASA-SM,~~ **a firewall device located at each of the State Data Centers (Robert E. Lee and Eastwood location)** to ~~have it~~ logically **insulate and isolate the DOR network and the DOR MARS project network from the remainder of the State network.** ~~bound in our DOR network~~**.** Timeline for completion is uncertain.

The following questions were submitted to ITS and are being presented as they were submitted, except to remove any reference to a specific vendor. This information should assist you in formulating your response.

Question 1: Section 6.4 states "Vendor's solution must include a fully managed Intrusion Detection/Prevention Service and System (IDS/IPS). For clarification, are the vendors being asked to provide the IDS/IPS technology in addition to the monitoring and management service?

Response: Yes, that is correct.

Question 1a: How many locations will require Source Fire technology deployment?

Board Members - Thomas A. Wicker, Chairman • June Songy, Vice-Chairman • D.Shane Loper • Rodney Pearson • J. Keith Van Camp
Legislative Advisors - Senator Sampson Jackson, II • Representative Gary V. Staples

Response: **Two (2), one for each logical network segment as described in section 5.2.1**

Question 1b: For each location, how many network segments will be monitored?

Response: **DOR network is logically partitioned such that there are only two (2) network segments to be monitored, as described in section 5. All DOR remote locations described in section 5.4 are logically behind the single network firewall described in section 5.2.1. Thus, the DOR network including headquarters and eight (8) remote locations is considered a single network segment for monitoring purposes. The second network segment to be monitored is described in section 5.2.1 as the DOR servers that are hosted in the State Data Center that make up part of the DOR MARS project.**

Question 2: What is the aggregate bandwidth throughput of the segments to be monitored for each location?

Response: **DOR's total aggregate bandwidth into and out of the DOR headquarters is 500 Mbps, the assumption would be that 500 Mbps would be the total monitoring load for each network segment.**

Question 2a: Copper or Fiber connections?

Response: **Copper is preferred.**

Question 2b: 1Gbps, 10Gbps connection?

Response: **1Gbps is preferred.**

Question 2c: Inline IPS or non-inline (passive)?

Response: **DOR would prefer Inline IPS. Vendor should propose as Vendor deems appropriate and justify if non-inline (passive).**

Question 3: Section 6.6.9.1 states IRS Publication 1075 requirements stipulate seven (7) years retention for certain logs. Is there currently any log management solution in place for long term storage of audit records as described in AU-4 and AU-11?

Response: **No, DOR is not currently capturing or storing logs that are within scope of this proposal.**

Question 3a: Is there any requirement for the log management solution to be on-site or off-site?

Response: **Provided that the requirement of section 5.2.1 is adhered to and met by the solution, the preference would be for offsite management. This prohibition of packet captures is an IRS Publication 1075 (indirect) requirement.**

Question 3b: Does the log management solution need to be fully managed by the provider?

Response: **Yes, DOR would prefer to have a fully managed solution.**

Question 4: For vulnerability scanning, approximately how many internal servers would be in scope?

Response: The Cost Information Form specifies 20 devices. Vendor should propose a unit price and provide details for adding and removing servers to / from scope for vulnerability scanning.

Question 5: For vulnerability scanning, approximately how many externally reachable servers would be in scope?

Response: The only externally accessible DOR server that is in scope is our web server, which exists in a DMZ defined in the ASA described in section 5.2.1.

Question 6: Section 6.6 specifies requirements for SIEM log correlation and monitoring. Was this intended to be separate, and in addition to, the 20 servers specified for real-time 24x7 security log monitoring in Section 6.9?

Response: The Cost Information Form specifies 20 devices. Vendor should propose a unit price and provide details for adding and removing servers to / from scope for SIEM.

Question 7: For SIEM log monitoring (page 11), approximately how many servers would you like to collect logs for?

Response: The Cost Information Form specifies 20 devices. Vendor should propose a unit price and provide details for adding and removing servers to / from scope for SIEM.

Question 8: Under SIEM requirements, section 6.6.8, requires the ability to "search and browse original log data". Does this apply only to security related logs and events, or all raw log data (non-security related log data) from monitored systems as well?

Response: DOR would prefer all raw log data. Vendor should propose as Vendor deems appropriate and justify if only security related logs and events.

Question 9: Section 6.9.4 requests optional pricing for Raw Log Storage. Approximately how many systems/servers would be in scope for raw log storage?

Response: All logs collected in the course of fulfilling the requirements of this proposal would be in scope. This includes approximately 17 network switch "stacks", 225 servers, 2 firewall contexts, 1000 network endpoints other than servers, plus miscellaneous other network devices.

LOC responses are due April 24, 2015, at 3:00 p.m. (Central Time).

If you have any questions concerning the information above or if we can be of further assistance, please contact Patti Irgens at 601-432-8223 or via email at Patti.Irgens@its.ms.gov.

cc: ITS Project File Number 41784